

## Sigurnosni nedostaci unutar programskog paketa OpenSSL



U radu programskog paketa openssl za operacijski sustav **Debian** otkrivena su dva sigurnosna propusta. **OpenSSL** omogućuje implementaciju **SSL** (eng. *Secure Sockets Layer*) i **TLS** (eng. *Transport Layer Security*) sigurnosnih protokola te pruža osnovnu kriptografsku podršku.

Prvi propust je posljedica pogreške tijekom ponovne razmjene parametara veze unutar postojeće **TLS** sesije. Drugi propust je uzrokovan mogućnošću izmjene skupa kriptografskih algoritama sesije. Napadaču je omogućeno izvodjenje **MitM** (eng. *Man-in-the-Middle*) napada i prikupljanje podataka unutar pojedinih sesija.

Ove ranjivosti imaju oznake: **CVE-2009-3555**, **CVE-2010-4180** i **DSA-2141-1**.

Ranjivosti su ispravljene u paketu openssl verzije **0.9.8g-15+lenny11** za **Debian lenny**.

Novo pakete za **Debian** možete instalirati na uobičajeni način:

```
apt-get update
```

```
apt-get upgrade
```

Ako želite instalirati samo ove pakete:

```
apt-get update
```

```
apt-get -y install openssl libssl0.9.8
```

Više informacija na:

<http://www.debian.org/security/2011/dsa-2141> [1]

CARNet, Grupa za izradu paketa

[paketi@carnet.hr](mailto:paketi@carnet.hr)

<http://paketi.carnet.hr/> [2]

pon, 2011-01-10 08:43 - Toni Pralas **Vijesti:** [Sigurnosni propusti](#) [3]

**Kategorije:** [Sigurnost](#) [4]

**Vote:** 0

No votes yet

**Source URL:** <https://sysportal.carnet.hr/node/805>

### Links

- [1] <http://www.debian.org/security/2011/dsa-2141>
- [2] <http://paketi.carnet.hr/>
- [3] <https://sysportal.carnet.hr/taxonomy/term/14>
- [4] <https://sysportal.carnet.hr/taxonomy/term/30>